



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,119	12/22/2003	W. Carey Bunn	END920030045US1	7503
46583	7590	04/28/2008		
GREENBLUM & BERNSTEIN, P.L.C. 1950 ROLAND CLARKE PLACE RESTON, VA 20191				
EXAMINER SCHMIDT, KARI L				
ART UNIT		PAPER NUMBER		
2139				
NOTIFICATION DATE		DELIVERY MODE		
04/28/2008		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

gbpatent@gbpatent.com

pto@gbpatent.com



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/743,119
Filing Date: December 22, 2003
Appellant(s): BUNN ET AL.

Andrew M. Calderon
Registration No. 38,093
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 19-February-2008 appealing from the Office action mailed 18-September-2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2003/0028803

Bunker, V et al.

2-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Bunker, V et al. (US 2003/0028803 A1).

Claim 1

Bunker discloses a method for checking network perimeter security, said method comprising the steps of: reviewing security of a network perimeter architecture; reviewing security of data processing devices that transfer data across the perimeter of the network; reviewing security of applications that transfer data across said perimeter;

and reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and generating a report concerning security of said perimeter based upon all of the reviewing steps (see at least, [0010]: "the preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions, external vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, gaining a true view of risk level without affecting customer operations. This assessment may be performed over the internet for domestic and worldwide corporations." [0012]: "the preferred embodiment includes a test center and one or more testers. The functionality of the test center may be divided into several subsystem components, possibly including a database, a command engine, a gateway, a report generator, and early warning generator and a repository master copy.").

Claim 2

Bunker discloses the method as set forth in claim 1 further comprising the step of reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter (see at least, [0122]: "Each Tester 502 may be pre-configured in-house and designed for remote administration. Therefore, it may be that no peripherals (e.g., keyboard, monitor, mouse, floppies, CD-ROM drives, etc.) are enabled while the Tester 502 is in the field. An exception might be an out-of-band, dial-up modem that

might feature strong encryption for authentication, logging, and dial-back capabilities to limit unauthorized access. This modem may be used, for example, in emergencies when the operating system is not completing its bootstrap and may be audited on a continuous basis. This may limit the need for "remote-hands" (e.g., ISP employees) to have system passwords, and may reduce the likelihood of needing a lengthy on-site trip. Other physical security methods, such as locked computer cases, may be implemented. One example might be a locked case that would, upon unauthorized entry, shock the hardware and render the components useless." [0125]: "Any username and password combination is susceptible to compromise, so an alternative is to not use passwords. An option is that only the administrator account has a password and that account can only be logged on locally (and not for example through the Internet) via physical access or the out-of-band modem. In this scenario, all other accounts have no passwords. Access would be controlled by means of public/private key technology that provides identification, authentication, and non-reputability of the user.").

Claim 3

Bunker discloses the method as set forth in claim 1 further comprising the step of reviewing security of data processing devices that authorize computers or users outside of said perimeter that request to access an application within said perimeter (see at least, [0122]: "Each Tester 502 may be pre-configured in-house and designed for remote administration. Therefore, it may be that no peripherals (e.g., keyboard, monitor, mouse, floppies, CD-ROM drives, etc.) are enabled while the Tester 502 is in

the field. An exception might be an out-of-band, dial-up modem that might feature strong encryption for authentication, logging, and dial-back capabilities to limit unauthorized access. This modem may be used, for example, in emergencies when the operating system is not completing its bootstrap and may be audited on a continuous basis. This may limit the need for "remote-hands" (e.g., ISP employees) to have system passwords, and may reduce the likelihood of needing a lengthy on-site trip. Other physical security methods, such as locked computer cases, may be implemented. One example might be a locked case that would, upon unauthorized entry, shock the hardware and render the components useless." [0123]: "Until the integrity of Tester 502 may be verified by an outside source, it may be the case that no communication with the device will be trusted and the device may be marked as suspect. Confidence in integrity may be improved by several means. First of all, Tester's 502 arsenals of tools 514, both proprietary and open source, may be contained on encrypted file systems. An encrypted file system may be a "drive" that, while unmounted, appears to be just a large encrypted file. In that case, when the correct password is supplied, the operating system would mount the file as a useable drive. The may prevent for example an unauthorized attacker with physical access to the Tester 502 from simply removing the drive, placing it into another machine and reading the contents. In that case, the only information an attacker might have access to might be the standard build of whatever operating system the Tester 502 happened to be running. If used, passwords may be random, unique to each Tester 502, and held in the Test Center 102. They may be changed from time to time, for example, on a bi-weekly basis.").

Claim 4

Bunker discloses the method as set forth in claim 1 wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of a web server, an e-mail server or an FTP server (see at least, [0116]-[0117], [0175]: "For the purposes of an internal assessment, several different appliances may be deployed on the customers network 1002. For example, for traveling consultants, a pre-configured laptop computer loaded with an instance of a Tester 502 might be shipped for deployment. For permanent, continuous assessment installations a dedicated, pre-configured device in either a thin, rack mountable form or desktop style tower might be shipped for deployment. In both cases the device might boot out-of-the-box to a simple, graphical, configuration editor. The editor's interface is a web browser that might point to the active web server on the local loop-back device. Since the web server may be running on the loop-back device, it may only be accessible by the local machine. Some options of local configurations might include, for example: IP Stack configuration, DNS information, default route table, push/pull connection to Test Center 102, account information, etc. Other options in the local configuration might include for example: IP diagnostics (Ping, Trace Route, etc.), DNS Resolutions, connections speed, hardware performance graphs, etc.") [0181] Overview 1400 in FIG. 14 illustrates a sample of the attack logic used by the preferred embodiment. Prior to the first "wave" 1410 of basic tests 516, an initial mapping 1402 records a complete inventory of services running on the target network 1002. An initial mapping 1402 discloses what systems 1102 are present, what ports are open (1404, 1406, and 1408) what services each system is

running, general networking problems, web or e-mail servers, whether the system's IP address is a phone number, etc. Basic network diagnostics might include whether a system can be pinged, whether a network connection fault exists, whether rerouting is successful, etc. For example, regarding ping, some networks have ping shut off at the router level, some at the firewall level, and some at the server level. If ping doesn't work, then attempt may be made to establish a handshake connection to see whether the system responds. If handshake doesn't work, then request confirmation from the system of receipt of a message that was never actually sent because some servers can thereby be caused to give a negative response. If that doesn't work, then send a message confirming reception of a message from the server that was not actually received because some servers can thereby be caused to give a negative response. Tactics like these can generate a significant amount of information about the customer's network of systems 1002.").

Claim 5

Bunker discloses the method as set forth in claim 1 further comprising the step of reviewing security of a server within said perimeter that provides data to said data processing devices that transfer data across the perimeter of said network (see at least, [0048] Database Subsystem Functionality; [0059], [0049]: "The Database 114 has multiple software modules and storage facilities 200 for performing different functions. The Database warehouses the raw data 214 collected by the Testers' 502 tests 516 from customers systems and networks 1002 and that data may be used by the Report

Generator 112 to produce different security reports 2230 for the customers. The raw data contained in the Database 114 can be migrated to any data format desired, for example by using ODBC to migrate to Oracle or Sybase. The type of data might include, for example, IP addresses, components, functions, etc. The raw data 214 may typically be fragmented and may not be easily understood until decoded by the Report Generator 110." [0052]: "The job scheduling module can initiate customer jobs at any time. It uses the customer profile information to tell the Command Engine what services the customer should receive, due to having been purchases, so that the Command Engine can conduct the appropriate range of tests." [0054]: "Every customer has a customer profile that may include description of the services the customer will be provided, the range of IP addresses the customer's network spans, who should receive the monthly reports, company mailing address, etc. The customer profile may be used by the Command Engine to conduct an appropriate set of tests on the customer's systems. The customer profile may be also used by the Report Generator to generate appropriate reports and send them to the appropriate destination. Customer Profile information includes that information discussed in this specification which would typically be provided by the Customer, such as IP addresses, services to be provided, etc.").

Claim 6

Bunker discloses the method as set forth in claim 1 wherein each of said reviews is performed by comparison to a security policy of an enterprise which owns or controls

said network (see at least, [0059], [0149], [0054]: "Every customer has a customer profile that may include description of the services the customer will be provided, the range of IP addresses the customer's network spans, who should receive the monthly reports, company mailing address, etc. The customer profile may be used by the Command Engine to conduct an appropriate set of tests on the customer's systems. The customer profile may be also used by the Report Generator to generate appropriate reports and send them to the appropriate destination. Customer Profile information includes that information discussed in this specification which would typically be provided by the Customer, such as IP addresses, services to be provided, etc." [0019] When a new security vulnerability may be announced on a resource like Bugtraq, the information may be added to the Vulnerability Library. Each vulnerability may be known to affect specific types of systems or specific versions of applications. The Vulnerability Library enables each vulnerability to be classified and cataloged. Entries in the Vulnerability Library might include, for example, vulnerability designation, vendor, product, version of product, protocol, vulnerable port, etc. Classification includes designating the severity of the vulnerability, while cataloging includes relating the vulnerability to the affected system(s) and/or application(s). The configuration of the new vulnerability may be compared to the customer's system network configuration compiled in the last test for the customer. If the new vulnerability is found to affect the customer systems or networks then a possibly detailed alert may be sent to the customer. The alert indicates which new vulnerability threatens the customer's network, possibly indicating specifically which machines may be affected and what to do in order

to correct the problem. Then, depending on the customer profile, after corrective measures are taken, the administrator can immediately use the system to verify the corrective measures in place or effectiveness of the corrective measures may be verified with the next scheduled security assessment.”).

Claim 7

Bunker discloses the method as set forth in claim 1 further comprising the step of determining said network perimeter (see at least, [0003], [0006], [0009], [0010], [0011]: “the preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions, external vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, gaining a true view of risk level without affecting customer operations. This assessment may be performed over the internet for domestic and worldwide corporations.”).

Claim 8

Bunker discloses the method as set forth in claim 7 wherein said network perimeter comprises entries and exits from said network (see at least, [0010]: “the preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions, external vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, gaining a true view of risk level without affecting customer operations. This assessment may be performed over the internet for domestic and

worldwide corporations.” [0059]: “The ability to perform performance metrics 208 comes from two places: (1) utilizing standard network utilities and methodologies, and (2) analysis of database 114 information. More sources of the ability to perform performance metrics 208 will become available over time. Current performance metrics 208 include, job completion timing, which is (1) time to complete an overall assessment (can be compared with type of assessment as well as size of job); (2) time to complete each Tool Suite 9 e.g., HTTP Suite 2318); (3) time to complete each wave of tests 516; and (3) time to complete each test 516. Also, assessment time per IP address/active nodes assessment time per type of service active on the machine. Tester 502 performance metrics 208 include, for example, resources available/used, memory, disk space, and processor. Gateway 118 performances metrics 208 include, for example, resources available/used, memory, disk space, and processor. Other performance metrics 208 include, for example, communication time between Tester 502 and Gateway 118 (latency), communication time between Gateway 118 and Tester 502 (network paths are generally different), and bandwidth available between Tester 502 and Gateway 118. Future performance metrics might include, Tester 502 usage, by operating system, by Network (Sprint, MCI, etc.), IP address on each Tester 502; test 516 effectiveness by operating system, by Network, by Tester 502; and Gateway 118/Distribution of tests across Testers 103.”; [0100], [0095], [0094], [0116], [0122], [0126]: “Security typically requires vigilance. Several processes may be in place to improve awareness of malicious activity that may be targeting an embodiment of the invention. Port Sentries and Log Sentries may be in place to watch and alert of any

suspicious activity and as a host-based intrusion detection system. Port Sentry is a simple, elegant, open source, public domain tool that is designed to alert administrators to unsolicited probes. Port sentry opens up several selected ports and waits for someone to connect. Typical choices of ports to open are services that are typically targeted by malicious attackers (e.g., ftp, sunRPC, Web, etc.). Upon connection, the program may do a variety of different things: drop route of the attacker to /dev/nul; add attacker to explicit deny list of host firewall; display a strong, legal warning; or run a custom retaliatory program. As such a strong response could lead to a denial of service issue with a valid customer; an alternative is to simply use it to log the attempt to the Tester 502 logs. Log sentry is another open source program that may be utilized for consolidation of log activity. It may check the logs every five minutes and email the results to the appropriate Internet address." [0181]).

Claim 9

Bunker discloses the method as set forth in claim 1 wherein said network perimeter comprises entries and exits from said network (see at least, [0010]: "the preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions, external vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, gaining a true view of risk level without affecting customer operations. This assessment may be performed over the internet for domestic and worldwide corporations." [0059]: "The ability to perform performance metrics 208 comes

from two places: (1) utilizing standard network utilities and methodologies, and (2) analysis of database 114 information. More sources of the ability to perform performance metrics 208 will become available over time. Current performance metrics 208 include, job completion timing, which is (1) time to complete an overall assessment (can be compared with type of assessment as well as size of job); (2) time to complete each Tool Suite 9 e.g., HTTP Suite 2318); (3) time to complete each wave of tests 516; and (3) time to complete each test 516. Also, assessment time per IP address/active nodes assessment time per type of service active on the machine. Tester 502 performance metrics 208 include, for example, resources available/used, memory, disk space, and processor. Gateway 118 performances metrics 208 include, for example, resources available/used, memory, disk space, and processor. Other performance metrics 208 include, for example, communication time between Tester 502 and Gateway 118 (latency), communication time between Gateway 118 and Tester 502 (network paths are generally different), and bandwidth available between Tester 502 and Gateway 118. Future performance metrics might include, Tester 502 usage, by operating system, by Network (Sprint, MCI, etc.), IP address on each Tester 502; test 516 effectiveness by operating system, by Network, by Tester 502; and Gateway 118/Distribution of tests across Testers 103.”; [0100], [0095], [0094], [0116], [0122], [0126]: “Security typically requires vigilance. Several processes may be in place to improve awareness of malicious activity that may be targeting an embodiment of the invention. Port Sentries and Log Sentries may be in place to watch and alert of any suspicious activity and as a host-based intrusion detection system. Port Sentry is a

simple, elegant, open source, public domain tool that is designed to alert administrators to unsolicited probes. Port sentry opens up several selected ports and waits for someone to connect. Typical choices of ports to open are services that are typically targeted by malicious attackers (e.g., ftp, sunRPC, Web, etc.). Upon connection, the program may do a variety of different things: drop route of the attacker to /dev/nul; add attacker to explicit deny list of host firewall; display a strong, legal warning; or run a custom retaliatory program. As such a strong response could lead to a denial of service issue with a valid customer, an alternative is to simply use it to log the attempt to the Tester 502 logs. Log sentry is another open source program that may be utilized for consolidation of log activity. It may check the logs every five minutes and email the results to the appropriate Internet address." [0181]).

Claim 10

Bunker discloses the method as set forth in claim 1 wherein the steps of reviewing security of a network perimeter, reviewing security of data processing devices that transfer data across the perimeter of the network, and reviewing vulnerability of applications or data processing devices within said perimeter from entities outside of said perimeter are performed at least in part with a respective program tool (see at least, [0010]: "the preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions, external vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, gaining a true view of risk level without affecting customer operations. This assessment may be performed over the

internet for domestic and worldwide corporations." [0012]: " the preferred embodiment includes a test center and one or more testers. The functionality of the test center may be divided into several subsystem components, possibly including a database, a command engine, a gateway, a report generator, and early warning generator and a repository master copy." [0054]: "Every customer has a customer profile that may include description of the services the customer will be provided, the range of IP addresses the customer's network spans, who should receive the monthly reports, company mailing address, etc. The customer profile may be used by the Command Engine to conduct an appropriate set of tests on the customer's systems. The customer profile may be also used by the Report Generator to generate appropriate reports and send them to the appropriate destination. Customer Profile information includes that information discussed in this specification which would typically be provided by the Customer, such as IP addresses, services to be provided, etc." [0019] When a new security vulnerability may be announced on a resource like Bugtraq, the information may be added to the Vulnerability Library. Each vulnerability may be known to affect specific types of systems or specific versions of applications. The Vulnerability Library enables each vulnerability to be classified and cataloged. Entries in the Vulnerability Library might include, for example, vulnerability designation, vendor, product, version of product, protocol, vulnerable port, etc. Classification includes designating the severity of the vulnerability, while cataloging includes relating the vulnerability to the affected system(s) and/or application(s). The configuration of the new vulnerability may be compared to the customer's system network configuration compiled in the last test for

the customer. If the new vulnerability is found to affect the customer systems or networks then a possibly detailed alert may be sent to the customer. The alert indicates which new vulnerability threatens the customer's network, possibly indicating specifically which machines may be affected and what to do in order to correct the problem. Then, depending on the customer profile, after corrective measures are taken, the administrator can immediately use the system to verify the corrective measures in place or effectiveness of the corrective measures may be verified with the next scheduled security assessment.”).

Claim 11

Bunker discloses the method as set forth in claim 1 wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of data processing devices accessed by users outside of said perimeter (see at least, [0054]: “Every customer has a customer profile that may include description of the services the customer will be provided, the range of IP addresses the customer's network spans, who should receive the monthly reports, company mailing address, etc. The customer profile may be used by the Command Engine to conduct an appropriate set of tests on the customer's systems. The customer profile may be also used by the Report Generator to generate appropriate reports and send them to the appropriate destination. Customer Profile information includes that information discussed in this specification which would typically be provided by the Customer, such as IP addresses, services to be provided, etc.” [0122]: “Each Tester 502 may be pre-configured in-house

Art Unit: 2132

and designed for remote administration. Therefore, it may be that no peripherals (e.g., keyboard, monitor, mouse, floppies, CD-ROM drives, etc.) are enabled while the Tester 502 is in the field. An exception might be an out-of-band, dial-up modem that might feature strong encryption for authentication, logging, and dial-back capabilities to limit unauthorized access. This modem may be used, for example, in emergencies when the operating system is not completing its bootstrap and may be audited on a continuous basis. This may limit the need for "remote-hands" (e.g., ISP employees) to have system passwords, and may reduce the likelihood of needing a lengthy on-site trip. Other physical security methods, such as locked computer cases, may be implemented. One example might be a locked case that would, upon unauthorized entry, shock the hardware and render the components useless." [0125]: "Any username and password combination is susceptible to compromise, so an alternative is to not use passwords. An option is that only the administrator account has a password and that account can only be logged on locally (and not for example through the Internet) via physical access or the out-of-band modem. In this scenario, all other accounts have no passwords. Access would be controlled by means of public/private key technology that provides identification, authentication, and non-reputability of the user.).

Claim 12

Bunker discloses the method as set forth in claim 1, wherein the reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points (see at least, [0073]).

Claim 13

Bunker discloses the method as set forth in claim 12, wherein the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises: testing control points with port scans; and testing control points with penetration tests (see at least, [0094-0095])

Claim 14

Bunker discloses the method as set forth in claim 1, further comprising: performing a policy review of an enterprise which owns or controls said network; defining review parameters based upon the policy review; and utilizing the review parameters to perform each of: the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (see at least, (see at least, [0010-0012], [0059], [0149], [0054]: "Every customer has a customer profile that may include description of the services the customer will be provided, the range of IP addresses the customer's network spans, who should receive the monthly reports, company mailing address, etc. The customer profile may be used by the Command Engine to conduct an appropriate set of tests on the customer's systems. The customer profile may be also used by the Report Generator to generate appropriate reports and send them to the appropriate destination. Customer Profile information

includes that information discussed in this specification which would typically be provided by the Customer, such as IP addresses, services to be provided, etc.” [0019]

When a new security vulnerability may be announced on a resource like Bugtraq, the information may be added to the Vulnerability Library. Each vulnerability may be known to affect specific types of systems or specific versions of applications. The Vulnerability Library enables each vulnerability to be classified and cataloged. Entries in the Vulnerability Library might include, for example, vulnerability designation, vendor, product, version of product, protocol, vulnerable port, etc. Classification includes designating the severity of the vulnerability, while cataloging includes relating the vulnerability to the affected system(s) and/or application(s). The configuration of the new vulnerability may be compared to the customer's system network configuration compiled in the last test for the customer. If the new vulnerability is found to affect the customer systems or networks then a possibly detailed alert may be sent to the customer. The alert indicates which new vulnerability threatens the customer's network, possibly indicating specifically which machines may be affected and what to do in order to correct the problem. Then, depending on the customer profile, after corrective measures are taken, the administrator can immediately use the system to verify the corrective measures in place or effectiveness of the corrective measures may be verified with the next scheduled security assessment.”).

Claim 15

Bunker discloses the method as set forth in claim 1, wherein: the reviewing security of a network perimeter architecture comprises receiving review parameters from a policy review and generating test cases; the reviewing security of data processing devices that transfer data across the perimeter of the network comprises receiving the review parameters, receiving the test cases, and performing the test cases; the reviewing security of applications that transfer data across said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases; and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases (see at least, [0010-0012], [0054], [0069-0083], [0095]).

Claims 16-20

The computer program product and system claims are one of the same therefore rejected for the same reason as the method claims 1-15 above.

(10) Response to Argument

With respect to the argument directed to claims 1, 3-5 and 7-11:

The applicant argues Bunker fails to disclose reviewing security of a network perimeter architecture; reviewing security of data processing devices that transfer data across the perimeter of the network; reviewing security of applications that transfer data across said perimeter; reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and generating a report concerning security of said perimeter based upon all of the reviewing steps.

The examiner notes Bunker discloses reviewing security of a network perimeter architecture (see at least, [0100]-[0102], [0126], [0181], [0197] and FIG. 17: the examiner notes [0181]: an initial mapping records a complete inventory of services running on a target network... and what ports are open); reviewing security of data processing devices that transfer data across the perimeter of the network (see at least, [0181]: the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers... router level and firewall level); reviewing security of applications that transfer data across said perimeter (see at least, [0181]: the examiner notes the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers...); reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (see at least, [0182]: the examiner notes vendor specific vulnerabilities); and generating a report concerning security of said perimeter based

upon all of the reviewing steps (see at least, [0204]-[0205]: the examiner notes a report generator generates a report about the systems profile, port utilization, and security vulnerabilities...).

The examiner notes a port scan and the state returned [0100]-[0102] perform a mapping of the given ports of the network [0181] and the monitoring of ports (e.g. Port Sentry), alert to unsolicited probes for suspicious activity concerning someone trying to connect to the given network [0126]), which would be reviewing a network perimeter architecture of the given network. Further the examiner notes pinging of router level and firewall level [0181] and the establishment of a handshake [0181], which would be the transfer of data across the perimeter of the network. The examiner notes looking for vendor specific vulnerabilities [0181] of the services (e.g. web or e-mail [0180]) would be reviewing security of applications and vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter. Finally the examiner notes a report generator generates a report about the systems profile, port utilization, and security vulnerabilities [0204]-[0205], which would be a generating a report based of the item reviewed. The examiner notes the following sections noted show the reviewing of the network perimeter, reviewing security of data processing devices, applications that transfer data across said perimeter; reviewing vulnerability of applications; and generating a report concerning security of said perimeter based upon all of the reviewing steps. The examiner notes under a broad but reasonable interpretation each of the claim limitations are disclosed in Bunker, therefore this argument is not persuasive.

With respect to the argument directed to claim 2:

The applicant argues Bunker fails to disclose reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter.

The examiner notes Bunker discloses reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter (see at least, [0126] and [0128]: the examiner notes a Log Sentry is used for consolidation of log activity). The examiner interprets from the following sections from Bunker, that under the broadest reasonable interpretation, Bunker discloses the claimed invention. The examiner notes a Log Sentry would log activity concerning access within the network and the applications within the network perimeter [0126] and further the examiner notes that users that which to access applications within the network perimeter would have to be authenticated by log-in or the use of public/private key technology in order to authenticate a users identity for access [0128], which would be reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter. The examiner notes under a broad but reasonable interpretation each of the claim limitations are disclosed in Bunker, therefore this argument is not persuasive.

With respect to argument directed to claim 6:

The applicant argues Bunker fails to disclose each of said reviews is performed by comparison to a security policy of an enterprise which owns or controls said network.

The examiner notes Bunker discloses each of said reviews is performed by comparison to a security policy of an enterprise which owns or controls said network (see at least, [0054] and [0118]). The examiner interprets from the following sections from Bunker, that under the broadest reasonable interpretation, Bunker discloses the claimed invention. The examiner notes a customer profile contains descriptions of the services the customer is provided, further the examiner notes the profile is used to conduct the proper tests in order to assess the given network and to generate the correct reports and send them to the correct entities [0054], which would be reviews is performed by comparison to a security policy of an enterprise which owns or controls said network. The examiner notes the customer profile acts as the security policy and further the adaptation of a policy module as seen in [0118], could also be used for policy information. The examiner notes under a broad but reasonable interpretation each of the claim limitations are disclosed in Bunker, therefore this argument is not persuasive.

With respect to the argument directed to claim 12:

The applicant argues Bunker fails to disclose the reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points.

The examiner notes Bunker discloses the reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points (see at least, [0054] and [0180]). The examiner interprets from the following sections from Bunker, that under the broadest reasonable interpretation, Bunker discloses the claimed invention. The examiner notes a customer profile contains descriptions of the services the customer is provided, further the examiner notes the profile is used to conduct the proper tests in order to assess the given network and to generate the correct reports and send them to the correct entities [0054] and further the examiner notes testing of given levels within the network router level, firewall level, and server level [0180], which would be reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points. The examiner notes within the network arts, control points are known as components that allow access within the networks, e.g. firewall or VPN. Therefore the testing of a control point or non-control point would be based on devices that transfer data across the network known (e.g. Router, Firewall, Server) [0180]). Further the examiner notes that the testing of the "control/non-control points" of Firewall/Filtering Rules would be conducted and have a report generated based on the results [0017]). The examiner notes under a broad but reasonable interpretation each of the claim limitations are disclosed in Bunker, therefore this argument is not persuasive.

With respect to the argument directed to claim 13:

The applicant argues Bunker fails to disclose the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises: testing control points with port scans; and testing control points with penetration tests.

The examiner notes Bunker discloses the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises: testing control points with port scans (see at least, [0095] and [0100]-[0102]); and testing control points with penetration tests (see at least, [0095]) and [0180]-[0182]). The examiner notes that a port scan is used as a control point test and further a cgi-scanner [0095] or reviewing of security holes [0181] would be a control point test for penetration. The examiner notes under a broad but reasonable interpretation each of the claim limitations are disclosed in Bunker, therefore this argument is not persuasive.

With respect to the argument directed to claim 14:

The applicant argues Bunker fails to disclose performing a policy review of an enterprise which owns or controls said network; defining review parameters based upon the policy review; and utilizing the review parameters to perform each of: the reviewing security of a network perimeter architecture , the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter.

The examiner notes Bunker discloses performing a policy review of an enterprise which owns or controls said network (see at least, [0054] and [0118]); defining review parameters based upon the policy review (see at least, [0054] and [0118]); and utilizing the review parameters to perform each of: the reviewing security of a network perimeter architecture (see at least, [0100]-[0102], [0126], [0181], [0197] and FIG. 17: the examiner notes [0181]: an initial mapping records a complete inventory of services running on a target network... and what ports are open), the reviewing security of data processing devices that transfer data across the perimeter of the network (see at least, [0181]: the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers... router level and firewall level), the reviewing security of applications that transfer data across said perimeter (see at least, [0181]: the examiner notes the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers...), and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (see at least, [0182]: the examiner notes vendor specific vulnerabilities). The examiner interprets from the following sections from Bunker, that under the broadest reasonable interpretation, Bunker discloses the claimed invention. The examiner notes a customer profile contains descriptions of the services the customer is provided, further the examiner notes the profile is used to conduct the proper tests in order to assess the given network and to generate the correct reports and send them to the correct entities [0054], which would be performing a policy review

of an enterprise which owns or controls said network and defining review parameters based upon the policy review. The examiner notes the customer profile acts as the security policy and further the adaptation of a policy module as seen in [0118], could also be used for policy information. The examiner notes a port scan and the state returned [0100]-[0102] perform a mapping of the given ports of the network [0181] and the monitoring of ports (e.g. Port Sentry), alert to unsolicited probes for suspicious activity concerning someone trying to connect to the given network [0126]), which would be reviewing a network perimeter architecture of the given network. Further the examiner notes pinging of router level and firewall level [0181] and the establishment of a handshake [0181], which would be the transfer of data across the perimeter of the network. The examiner notes looking for vendor specific vulnerabilities [0181] of the services (e.g. web or e-mail [0180]) would be reviewing security of applications and vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter. Finally the examiner notes a report generator generates a report about the systems profile, port utilization, and security vulnerabilities [0204]-[0205], which would be a generating a report based of the item reviewed. The examiner notes the following sections noted show the reviewing of the network perimeter, reviewing security of data processing devices, applications that transfer data across said perimeter; reviewing vulnerability of applications; and generating a report concerning security of said perimeter based upon all of the reviewing steps. The examiner notes under a broad but reasonable interpretation each

of the claim limitations are disclosed in Bunker, therefore this argument is not persuasive.

With respect to the argument directed to claim 15:

The applicant argues Bunker fails to disclose the reviewing security of a network perimeter architecture comprises receiving review parameters from a policy review and generating test cases; the reviewing security of data processing devices that transfer data across the perimeter of the network comprises receiving the review parameters, receiving the test cases, and performing the test cases; the reviewing security of applications that transfer data across said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases; and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases.

The examiner notes Bunker discloses the reviewing security of a network perimeter architecture comprises receiving review parameters from a policy review and generating test cases (see at least, [0016], [0100]-[0102], [0126], [0181], [0197] and FIG. 17: the examiner notes [0181]: an initial mapping records a complete inventory of services running on a target network... and what ports are open); the reviewing security of data processing devices that transfer data across the perimeter of the network comprises receiving the review parameters, receiving the test cases, and performing the test cases (see at least, [0181]: the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is

running... web or e-mail servers... router level and firewall level); the reviewing security of applications that transfer data across said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases (see at least, [0181]: the examiner notes the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers...); and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases (see at least, [0182]: the examiner notes vendor specific vulnerabilities). The examiner interprets from the following sections from Bunker, that under the broadest reasonable interpretation, Bunker discloses the claimed invention. The examiner notes that that a "basic test" is test case and is used to simulate and iteratively test the customers system, which would be the generating of a test case and performing the test case for all the reviewing steps claimed. The examiner notes a port scan and the state returned [0100]-[0102] perform a mapping of the given ports of the network [0181] and the monitoring of ports (e.g. Port Sentry), alert to unsolicited probes for suspicious activity concerning someone trying to connect to the given network [0126]), which would be reviewing a network perimeter architecture of the given network. Further the examiner notes pinging of router level and firewall level [0181] and the establishment of a handshake [0181], which would be the transfer of data across the perimeter of the network. The examiner notes looking for vendor specific vulnerabilities [0181] of the services (e.g. web or e-mail [0180]) would be reviewing security of applications and

vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter. Finally the examiner notes a report generator generates a report about the systems profile, port utilization, and security vulnerabilities [0204]-[0205], which would be a generating a report based of the item reviewed. The examiner notes the following sections noted show the reviewing of the network perimeter, reviewing security of data processing devices, applications that transfer data across said perimeter; reviewing vulnerability of applications; and generating a report concerning security of said perimeter based upon all of the reviewing steps. The examiner notes under a broad but reasonable interpretation each of the claim limitations are disclosed in Bunker, therefore this argument is not persuasive.

With respect to the argument directed to claim 16:

The applicant argues that Bunker fails to disclose a computer program product comprising a computer usable medium having a computer readable program embodied in the medium, wherein the computer readable program when executed on a computing device is operable to cause the computing device to: review security of a network perimeter architecture; review security of data processing devices that transfer data across the perimeter of the network; review security of applications that transfer data across said perimeter; review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and generate a report concerning security of said perimeter based upon all said reviews.

The examiner notes Bunker discloses a computer program product comprising a computer usable medium having a computer readable program embodied in the medium, wherein the computer readable program when executed on a computing device is operable to cause the computing device to (see at least, [0048] and [0068]-[0069]): review security of a network perimeter architecture (see at least, [0100]-[0102], [0126], [0181], [0197] and FIG. 17: the examiner notes [0181]: an initial mapping records a complete inventory of services running on a target network... and what ports are open); review security of data processing devices that transfer data across the perimeter of the network (see at least, [0181]: the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers... router level and firewall level); review security of applications that transfer data across said perimeter (see at least, [0181]: the examiner notes the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers...); review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (see at least, [0182]: the examiner notes vendor specific vulnerabilities); and generate a report concerning security of said perimeter based upon all said reviews (see at least, [0204]-[0205]: the examiner notes a report generator generates a report about the systems profile, port utilization, and security vulnerabilities...). The examiner notes under a broad but reasonable interpretation each of the claim limitations are disclosed in Bunker, therefore this argument is not persuasive.

The examiner notes the database and command engine are a computer program product that executes on a computing device [0048] and [0068]), which perform the given tests. The examiner notes a port scan and the state returned [0100]-[0102] perform a mapping of the given ports of the network [0181] and the monitoring of ports (e.g. Port Sentry), alert to unsolicited probes for suspicious activity concerning someone trying to connect to the given network [0126]), which would be reviewing a network perimeter architecture of the given network. Further the examiner notes pinging of router level and firewall level [0181] and the establishment of a handshake [0181], which would be the transfer of data across the perimeter of the network. The examiner notes looking for vendor specific vulnerabilities [0181] of the services (e.g. web or e-mail [0180]) would be reviewing security of applications and vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter. Finally the examiner notes a report generator generates a report about the systems profile, port utilization, and security vulnerabilities [0204]-[0205], which would be a generating a report based of the item reviewed. The examiner notes the following sections noted show the reviewing of the network perimeter, reviewing security of data processing devices, applications that transfer data across said perimeter; reviewing vulnerability of applications; and generating a report concerning security of said perimeter based upon all of the reviewing steps. The examiner notes under a broad but reasonable interpretation each of the claim limitations are disclosed in Bunker, therefore this argument is not persuasive.

With respect to the argument directed to claim 17:

The applicant argues that Bunker fails to disclose the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter utilize review parameters defined in a policy review of an enterprise which owns or controls said network.

The examiner notes Bunker discloses the reviewing security of a network perimeter architecture (see at least, [0100]-[0102], [0126], [0181], [0197] and FIG. 17: the examiner notes [0181]: an initial mapping records a complete inventory of services running on a target network... and what ports are open); reviewing security of data processing devices that transfer data across the perimeter of the network (see at least, [0181]: the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers... router level and firewall level); reviewing security of applications that transfer data across said perimeter (see at least, [0181]: the examiner notes the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers...); reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (see at least, [0182]: the examiner notes vendor specific vulnerabilities) utilize review parameters defined in a policy review of an enterprise

which owns or controls said network (see at least, [0054] and [0118]). The examiner interprets from the following sections from Bunker, that under the broadest reasonable interpretation, Bunker discloses the claimed invention. The examiner notes a customer profile contains descriptions of the services the customer is provided, further the examiner notes the profile is used to conduct the proper tests in order to assess the given network and to generate the correct reports and send them to the correct entities [0054], which would be performing a policy review of an enterprise which owns or controls said network and defining review parameters based upon the policy review. The examiner notes the customer profile acts as the security policy and further the adaptation of a policy module as seen in [0118], could also be used for policy information. The examiner notes a port scan and the state returned [0100]-[0102] perform a mapping of the given ports of the network [0181] and the monitoring of ports (e.g. Port Sentry), alert to unsolicited probes for suspicious activity concerning someone trying to connect to the given network [0126]), which would be reviewing a network perimeter architecture of the given network. Further the examiner notes ping of router level and firewall level [0181] and the establishment of a handshake [0181], which would be the transfer of data across the perimeter of the network. The examiner notes looking for vendor specific vulnerabilities [0181] of the services (e.g. web or e-mail [0180]) would be reviewing security of applications and vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter. Finally the examiner notes a report generator generates a report about the systems profile, port utilization, and security vulnerabilities [0204]-[0205], which

would be a generating a report based of the item reviewed. The examiner notes the following sections noted show the reviewing of the network perimeter, reviewing security of data processing devices, applications that transfer data across said perimeter; reviewing vulnerability of applications; and generating a report concerning security of said perimeter based upon all of the reviewing steps. The examiner notes under a broad but reasonable interpretation each of the claim limitations are disclosed in Bunker, therefore this argument is not persuasive.

With respect to the argument directed to claims 18-19:

The applicant argues Bunker fails to disclose a system, comprising: a network having a perimeter; and a terminal connected to the network and arranged to: review security of a network perimeter architecture; review security of data processing devices that transfer data across the perimeter of the network; review security of applications that transfer data across said perimeter; review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and generate a report concerning security of said perimeter based upon all said reviews.

The examiner notes Bunker discloses a system, comprising: a network having a perimeter (see at least, [0100]-[0102], [0126], [0181], [0197] and FIG. 17: the examiner notes [0181]: an initial mapping records a complete inventory of services running on a target network... and what ports are open); and a terminal connected to the network and arranged to (see at least, [0088]): review security of a network perimeter architecture (see at least, [0100]-[0102], [0126], [0181], [0197] and FIG. 17: the

examiner notes [0181]: an initial mapping records a complete inventory of services running on a target network... and what ports are open); review security of data processing devices that transfer data across the perimeter of the network (see at least, [0181]: the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers... router level and firewall level); review security of applications that transfer data across said perimeter (see at least, [0181]: the examiner notes the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers...); review vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter see at least, [0182]: the examiner notes vendor specific vulnerabilities); and generate a report concerning security of said perimeter based upon all said reviews (see at least, [0204]-[0205]: the examiner notes a report generator generates a report about the systems profile, port utilization, and security vulnerabilities...). The examiner interprets from the following sections from Bunker, that under the broadest reasonable interpretation, Bunker discloses the claimed invention. The examiner notes a customer profile contains descriptions of the services the customer is provided, further the examiner notes the profile is used to conduct the proper tests in order to assess the given network and to generate the correct reports and send them to the correct entities [0054], which would be performing a policy review of an enterprise which owns or controls said network and defining review parameters based upon the policy review. The examiner notes the customer profile acts as the

security policy and further the adaptation of a policy module as seen in [0118], could also be used for policy information. The examiner notes a multiple testers [0088] and [0094] and Fig. 10, would have there own terminal (e.g. portal [0210]). The examiner notes a port scan and the state returned [0100]-[0102] perform a mapping of the given ports of the network [0181] and the monitoring of ports (e.g. Port Sentry), alert to unsolicited probes for suspicious activity concerning someone trying to connect to the given network [0126]), which would be reviewing a network perimeter architecture of the given network. Further the examiner notes pinging of router level and firewall level [0181] and the establishment of a handshake [0181], which would be the transfer of data across the perimeter of the network. The examiner notes looking for vendor specific vulnerabilities [0181] of the services (e.g. web or e-mail [0180]) would be reviewing security of applications and vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter. Finally the examiner notes a report generator generates a report about the systems profile, port utilization, and security vulnerabilities [0204]-[0205], which would be a generating a report based of the item reviewed. The examiner notes the following sections noted show the reviewing of the network perimeter, reviewing security of data processing devices, applications that transfer data across said perimeter; reviewing vulnerability of applications; and generating a report concerning security of said perimeter based upon all of the reviewing steps. The examiner notes under a broad but reasonable interpretation each of the claim limitations are disclosed in Bunker, therefore this argument is not persuasive.

With respect to the argument directed to claim 20:

The applicant argues Bunker fails to disclose each of the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter utilize review parameters defined in a policy review of an enterprise which owns or controls said network.

The examiner notes Bunker discloses each of the reviewing security of a network perimeter architecture (see at least, [0100]-[0102], [0126], [0181], [0197] and FIG. 17: the examiner notes [0181]: an initial mapping records a complete inventory of services running on a target network... and what ports are open); reviewing security of data processing devices that transfer data across the perimeter of the network (see at least, [0181]: the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers... router level and firewall level); reviewing security of applications that transfer data across said perimeter (see at least, [0181]: the examiner notes the examiner notes an initial mapping records a complete inventory of services running on a target network... services system is running... web or e-mail servers...); reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (see at least, [0182]: the examiner notes vendor specific

vulnerabilities) utilize review parameters defined in a policy review of an enterprise which owns or controls said network (see at least, [0054] and [0118]).

The examiner notes a customer profile contains descriptions of the services the customer is provided, further the examiner notes the profile is used to conduct the proper tests in order to assess the given network and to generate the correct reports and send them to the correct entities [0054], which would be performing a policy review of an enterprise which owns or controls said network and defining review parameters based upon the policy review. The examiner notes the customer profile acts as the security policy and further the adaptation of a policy module as seen in [0118], could also be used for policy information. The examiner notes a port scan and the state returned [0100]-[0102] perform a mapping of the given ports of the network [0181] and the monitoring of ports (e.g. Port Sentry), alert to unsolicited probes for suspicious activity concerning someone trying to connect to the given network [0126]), which would be reviewing a network perimeter architecture of the given network. Further the examiner notes pinging of router level and firewall level [0181] and the establishment of a handshake [0181], which would be the transfer of data across the perimeter of the network. The examiner notes looking for vendor specific vulnerabilities [0181] of the services (e.g. web or e-mail [0180]) would be reviewing security of applications and vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter. Finally the examiner notes a report generator generates a report about the systems profile, port utilization, and security vulnerabilities [0204]-[0205], which would be a generating a report based of the item

reviewed. The examiner notes the following sections noted show the reviewing of the network perimeter, reviewing security of data processing devices, applications that transfer data across said perimeter; reviewing vulnerability of applications; and generating a report concerning security of said perimeter based upon all of the reviewing steps.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Kari L. Schmidt

/Kari L Schmidt/
Examiner, Art Unit 2139

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/G. B./
Supervisory Patent Examiner, Art Unit 2132

Benjamin Lanier
/Benjamin E Lanier/
Primary Examiner, Art Unit 2132